



2016
DENVER 
5 - 7 October 2016

Locky Strike: Smoking the Locky Ransomware Code

Floser Bacurio Jr and Rommel Joven
Anti-Virus Analysts, FortiGuard Lion Team



FORTINET 

October 7, 2016

Cryptowall

What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall
More information about the encryption keys using RSA-2048 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. 3wzn5p2yiumh7akj.paypartnerstodo.com/g3tz2m
2. 3wzn5p2yiumh7akj.allepohelp.to.com/g3tz2m
3. 3wzn5p2yiumh7akj.bark1paypartners.com/g3tz2m
4. 3wzn5p2yiumh7akj.maverickpaypartners.com/g3tz2m

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. 3wzn5p2yiumh7akj.onion/g3tz2m ◀ Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

paypartnerstodo.com/g3tz2m	◀ Your Personal PAGE
3wzn5p2yiumh7akj.onion/g3tz2m	◀ Your Personal PAGE(using TOR)
g3tz2m	◀ Your personal code (if you open the site (or TOR 's) directly)

This one?

```
~==*~|||+=$=$**|$$_  
._~=_*-$_*+=+$||  
+*+._|  
~*++
```

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

1. <http://5n7y4yihircftc5.tor2web.org/ECCEADDE847A1F1A>
2. <http://5n7y4yihircftc5.onion.to/ECCEADDE847A1F1A>

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 5n7y4yihircftc5.onion.to/ECCEADDE847A1F1A
4. Follow the instructions on the site.

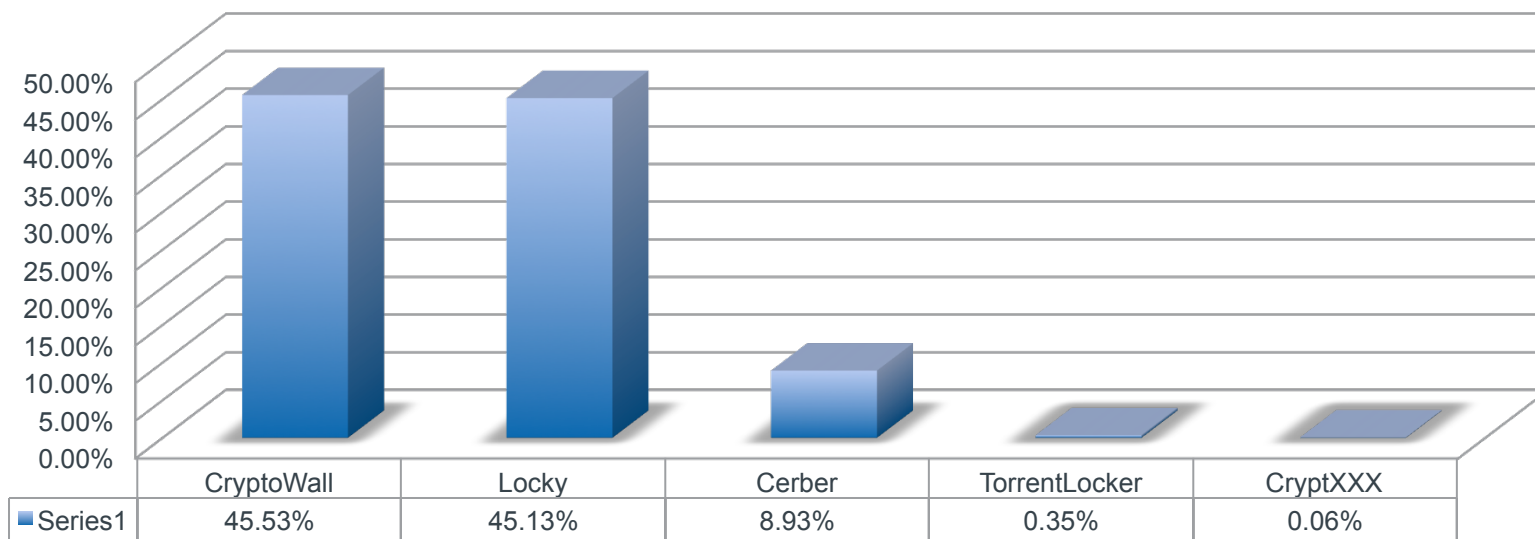
!!! Your personal identification ID: ECCEADDE847A1F1A !!!

```
*_|$|_=  
*=|~__
```

Prevalence: Global ransomware



Global Ransomware IPS Hits - February 19 to September 15 2016



Prevalence: Top countries

Locky Ransomware IPS Hits –
February 19 to September 15 2016

Locky-est

Total Hits: 36,314,789

US	11,858,085
FR	6,959,892
JP	3,071,596
KW	2,732,454
TW	1,338,216
AR	970,339
CL	890,784
PR	709,372
IT	556,602
IL	540,992

Prevalence: Affiliate program



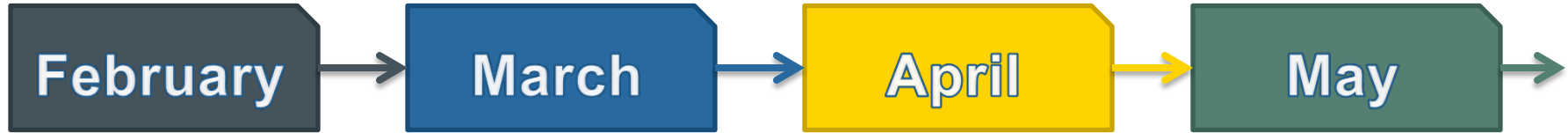
The following is a list of affiliate methods that have been observed:

affid	Method
1	Spam email containing an attached JavaScript, MS Office Macro downloader or Windows Script File
3	Spam email containing an attached JavaScript or Microsoft Office Macro downloader
5	Spam email containing an attached JavaScript downloader
13	Compromised sites that redirects to Nuclear or Neutrino Exploit Kit
15	Spam email containing an attached JavaScript or HTA downloader

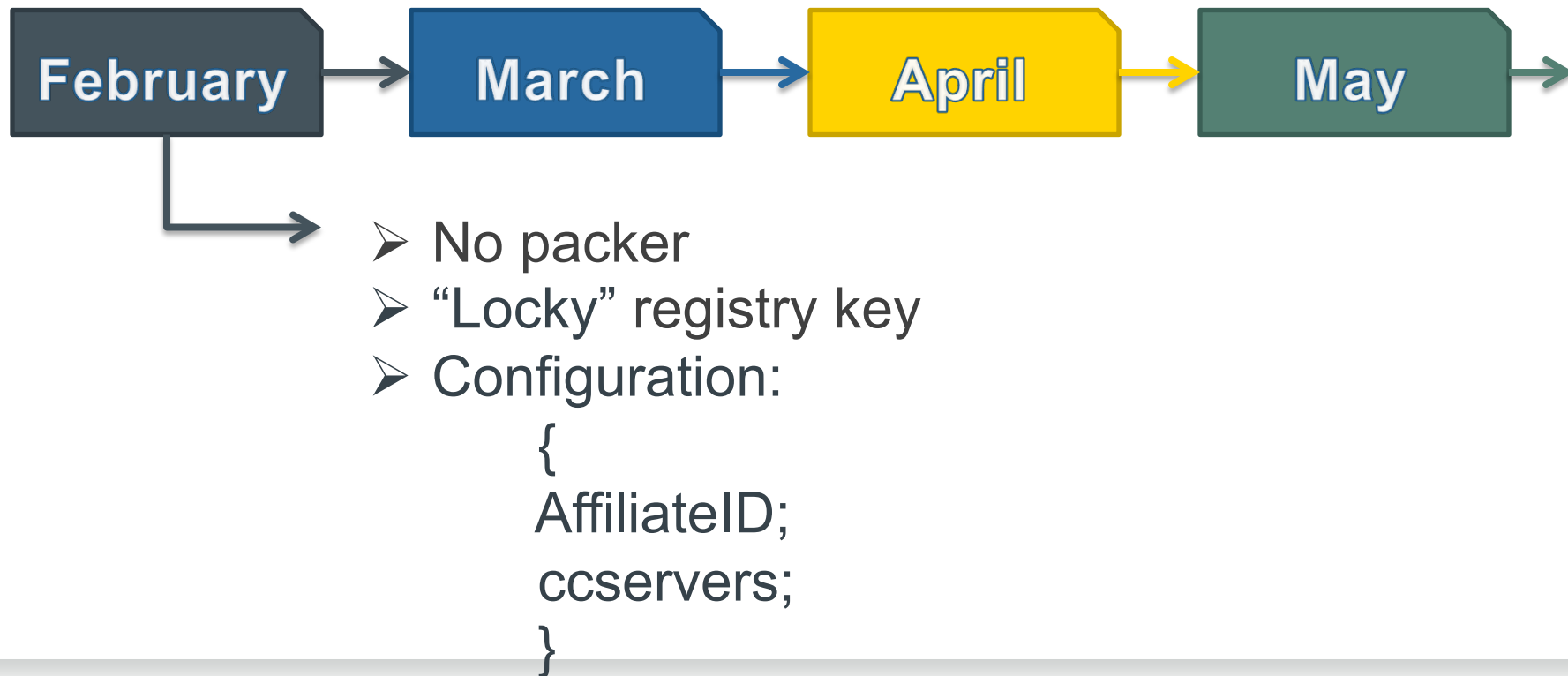


Locky Developments

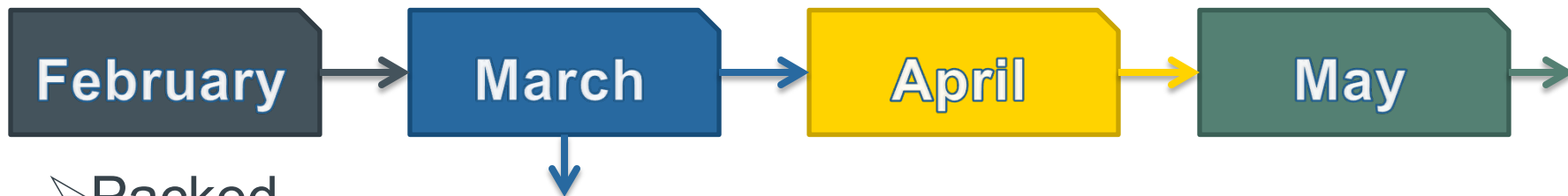
Timeline of Developments: 2016



Timeline of Developments: 2016



Timeline of Developments: 2016

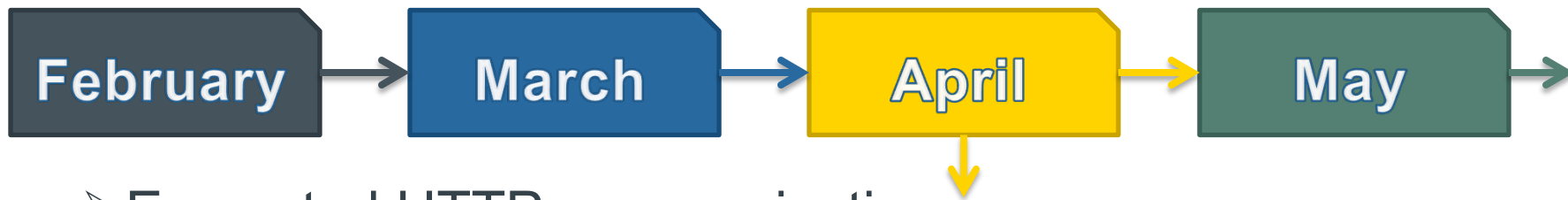


- Packed
- Registry key based on VolumeGUID
- Configuration(encrypted):

```
{  
  AffiliateID;  
  DGASeed;  
  delaySeconds;  
  FakeSvchost;  
  Persistence;  
  IgnoreRussian;  
  ccServers;  
}
```



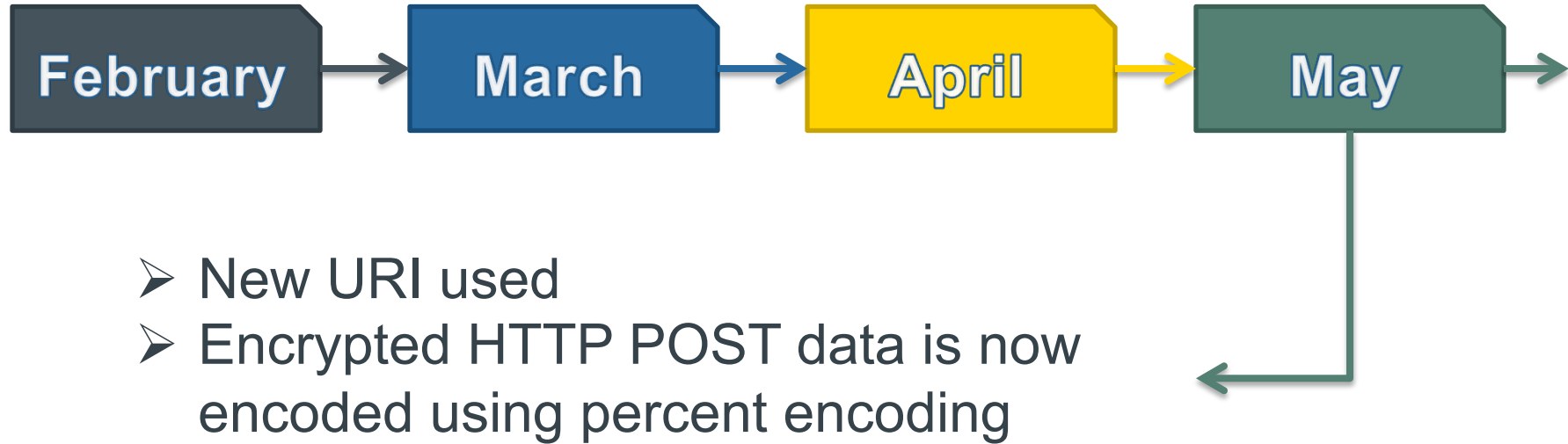
Timeline of Developments: 2016



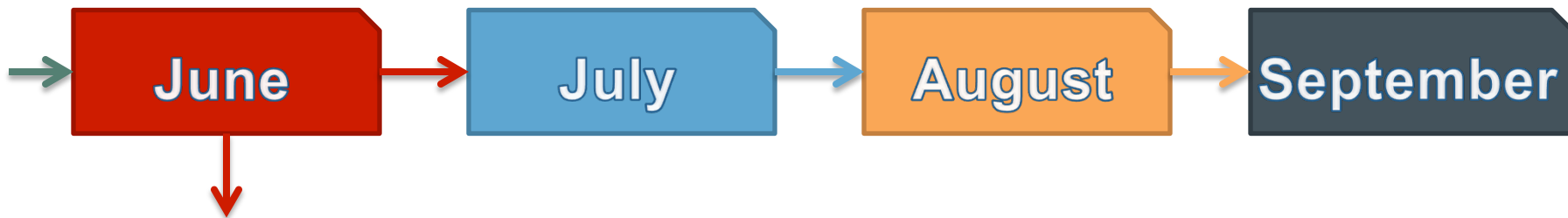
- Encrypted HTTP communication
- Configuration:

```
{  
  AffiliateID;  
  DGASeed;  
  delaySeconds;  
  FakeSvchost;  
  Persistence;  
  IgnoreRussian;  
  urlPath;  
  ccServers;  
}
```

Timeline of Developments: 2016



Timeline of Developments: 2016



- Requires argument. (e.g “123”, “321”)

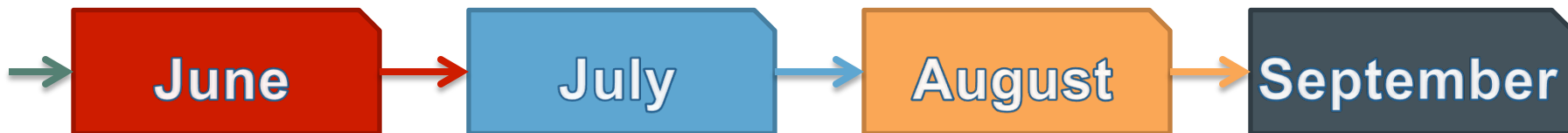
Cracking Locky's New Anti-Sandbox Technique

by  Floser Bacurio and Roland Dela Paz | Jun 30, 2016 | Filed in: Security Research

The last few weeks saw new variants of the Locky ransomware that employs a new anti-sandbox technique. from its JavaScript downloader in order to decrypt embedded malicious code and execute it properly. For example in the following manner:

```
sample.exe 123
```

Timeline of Developments: 2016



The Newest Online Threat – .Zepto Ransomware



TRIPWIRE GUEST AUTHORS

JUN 29, 2016

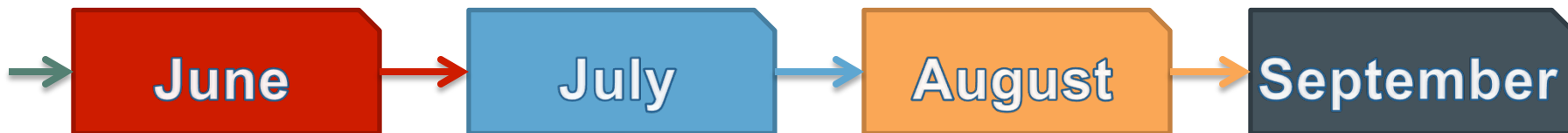
LATEST SECURITY NEWS



Zepto ransomware spam campaign surges with over 130,000 emails in 4 days

■ Hackers have used subject lines like 'financial report', 'documents copy' and others in efforts to lure in victims.

Timeline of Developments: 2016



- Offline Mode encryption

PCWorld
FROM IDG

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES

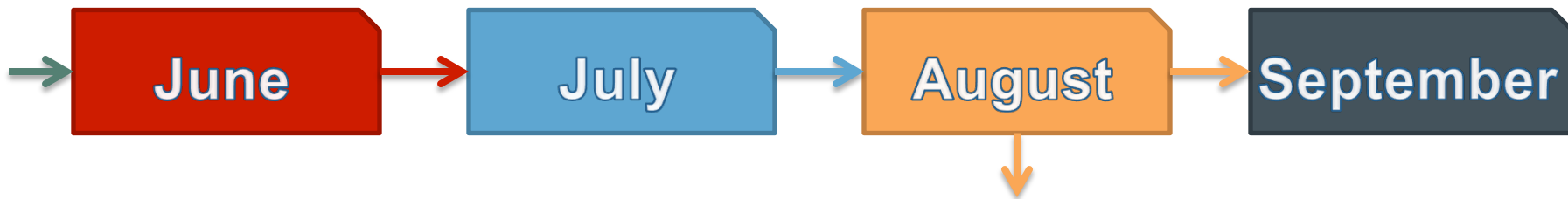
Privacy Encryption Antivirus

[Home](#) / [Security](#)

New Locky ransomware version can operate in offline mode

The program will start encrypting files even if it can't connect to a command-and-control server.

Timeline of Developments: 2016



[Subscribe \(Free\)](#) | [CISO Forum 2016](#)

[Malware & Threats](#) [Cybercrime](#) [Mobile & Wireless](#) [Risk & Compliance](#) [Security Architecture](#) [Management](#)

[Home](#) > [Malware](#)

Locky Ransomware Switches to DLLs for Distribution

By [SecurityWeek News](#) on August 26, 2016

[in](#) Share

49

[G+](#)

5

[Tweet](#)

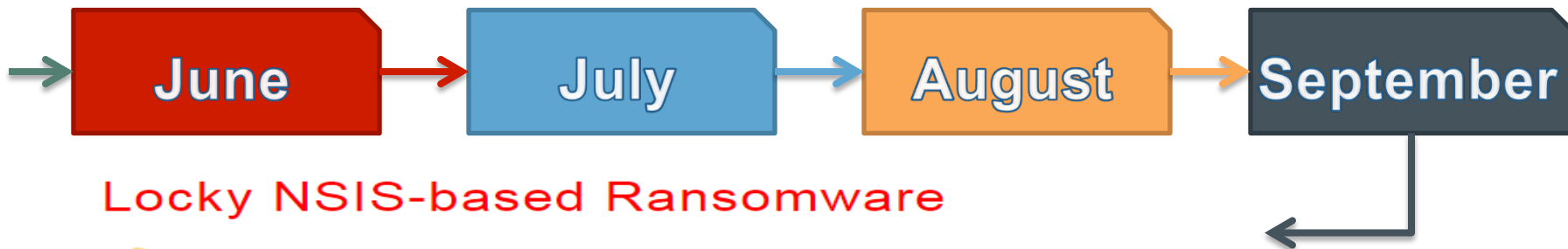
[f](#) Recommend

34

[RSS](#)

Locky, one of the most popular ransomware families at the moment, has changed its distribution method once again and is now using DLLs for infection, Cyren researchers warn.

Timeline of Developments: 2016



Locky NSIS-based Ransomware

by  Floser Bacurio Jr. and Kenny Yongjian Yang | Sep 12, 2016 | Filed in: [Security](#)

Over the last few months we saw that Locky's loader **uses** seed parameter without the correct parameter. Afterwards, we saw Locky **shift** itself from

Odin File Virus Ransomware Is Here!



TRIPWIRE GUEST AUTHORS

SEP 27, 2016 |

LATEST SECURITY NEWS



Technical Analysis

Configuration

Drop *svchost.exe*: 01
Skip: 00
Delay(Sleep)

DGA Seed
Affiliate ID

Autorun: 01
Skip: 00
Check RU: 01
Skip: 00
C&C offset

Address	Hex dump	ASCII
00850000	05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 00 01 2F	...i#...▲...☺
00850010	75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00	userinfo.php...
00850020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	8
00850030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	2
00850040	33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32	3.217.8.155,91.2
00850050	32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34	26.93.113,31.184
00850060	2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00	.197.126.....

Configuration

URI for its C&C

- main.php
- submit.php
- userinfo.php
- access.cgi
- /upload/_dispatch.php
- /php/upload.php
- /data/info.php
- /apache_handler.php

C&Cs

Address	Hex dump	ASCII
00850000	05 00 00 00 AD 23 00 00 1E 00 00 00 00 00 01 2F	#.....
00850010	75 73 65 72 69 6E 66 6F 2E 70 68 70 00 00 00 00	userinfo.php
00850020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00850030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38	8
00850040	33 2E 32 31 37 2E 38 2E 31 35 35 2C 39 31 2E 32	3.217.8.155,91.2
00850050	32 36 2E 39 33 2E 31 31 33 2C 33 31 2E 31 38 34	26.93.113,31.184
00850060	2E 31 39 37 2E 31 32 36 00 00 00 00 00 00 00 00	.197.126.....

Configuration



Address	Hex dump																ASCII
00850000	05	00	00	00	AD	23	00	00	1E	00	00	00	00	00	01	2F	..i#..▲.....☺✓
00850010	75	73	65	72	69	6E	66	6F	2E	70	68	70	00	00	00	00	userinfo.php.....
00850020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	8
00850030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	38	8
00850040	33	2E	32	31	37	2E	38	2E	31	35	35	2C	39	31	2E	32	3.217.8.155,91.2
00850050	32	36	2E	39	33	2E	31	31	33	2C	33	31	2E	31	38	34	26.93.113,31.184
00850060	2E	31	39	37	2E	31	32	36	00	00	00	00	00	00	00	00	.197.126.....

Configuration: Offline

Online mode

Address	Hex dump																ASCII
00850000	05	00	00	00	AD	23	00	00	1E	00	00	00	00	00	01	2F	⌨...!#...▲...☑
00850010	75	73	65	72	69	6E	66	6F	2E	70	68	70	00	00	00	00	userinfo.php...
00850020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00850030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	38	8
00850040	33	2E	32	31	37	2E	38	2E	31	35	35	2C	39	31	2E	32	3.217.8.155.91.2
00850050	32	36	2E	39	33	2E	31	31	33	2C	33	31	2E	31	38	34	26.93.113.31.184
00850060	2E	31	39	37	2E	31	32	36	00	00	00	00	00	00	00	00	.197.126.....

No DGA Seed

Offline mode

No C&C offset

Address	Hex dump																ASCII	
019A0000	03	00	00	00	00	00	00	00	27	00	00	00	00	00	00	01	00	♥.....'.....☹
019A0010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
019A0020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
019A0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
019A0040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
019A0050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
019A0060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

No C&Cs and URI

Configuration: Offline

Offline mode

Address	Hex dump	ASCII
019A0000	03 00 00 00 00 00 00 00 27 00 00 00 00 00 01 00	'.....
019A0010	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
019A0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
019A0030	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
019A0040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
019A0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
019A0060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Embedded Public RSA key

```
019A103F  r@...@...+@...ñ...RSA1...@...@...}v<^5=0...àUw%zn0%8<+||2j|n@j|P^~#
019A107F  |+=t2êiW+q.òã@u|á-±v<_r-étp>\W<<Gr!!U+ J%@.8Cv7$KW▲-S@.d i< .Lp9E
019A10BF  u]_ ;dgú-#akR#ó@ú\||ibæø#Ω jCæøeóQ0àq%uf\_-;_ö||u>íöû8P-|<A">€→\I
019A10FF  +Σ |M9-3vM≡u~u|▲| 73B@^nb|P0i♥7j>>z.OΣ>Jàa@M♥ZTéøB@#90→.JNj+|#?u1!!F
019A113F  ÷öæTEñ÷øFt@o.\hfe|&A♦1'|t\↓.....
```

Embedded Ransom Text

```
019A1493 0~.~.=!*~.=~-.$!$*!.~.$_-.. !!! IMPORTANT INFORMATION
019A14D3 !!!!!...All of your files are encrypted with RSA-2048 and AES-1
019A1513 28 ciphers...More information about the RSA and AES can be found
019A1553 here:... http://en.wikipedia.org/wiki/RSA_(cryptosystem)..
019A1593 http://en.wikipedia.org/wiki/Advanced_Encryption_Standard..
019A15D3 ..Decrypting of your files is only possible with the private key
019A1613 and decrypt program, which is on our secret server...To receive
019A1653 your private key follow one of the links:... 1. http://5n7y4y
019A1693 ihirccftc5.tor2web.org/FF00000000000000FF.. 2. http://5n7y4yihi
019A16D3 rccftc5.onion.to/FF00000000000000FF....If all of this addresses ar
019A1713 e not available, follow these steps:... 1. Download and instal
019A1753 l Tor Browser: https://www.torproject.org/download/download-easy
019A1793 .html.. 2. After a successful installation, run the browser a
019A17D3 nd wait for initialization... 3. Type in the address bar: 5n7
019A1813 y4yihirccftc5.onion/FF00000000000000FF.. 4. Follow the instruct
019A1853 ions on the site.....!!! Your personal identification ID: FF0000
019A1893 00000000FF !!!.....~+...=-_|-..|=+-|-_|~*~*..=-~~~ .....
```

Embedded HTML Ransom Text

```
019A37BE <a href="http://5n7y4yihircftc5.tor2web.org/FF00000000000000FF" t
019A37FE arget="_blank">http://5n7y4yihircftc5.tor2web.org/FF000000000000
019A383E 0FF</a><br /><span class='kqfldfq'>&nbsp;  </span><div class=owfbp
019A387E rnjid>qqsiz</div><span class='kqfldfq'>a</span><span class='kqfl
019A38BE dfq'>c</span><div class=owfbprnjid>wmdidtjxu</div><span class='k
019A38FE qfldfq'></span><div class=owfbprnjid>bkzgxnx</div>2.<span class=
```

Victim ID: Online



Locky creates a victim ID that needs to identify unique systems.

The victim ID is created from the following information:

- Volume GUID of the *WindowsDirectory*
- *MD5* hash of the GUID value

e.g. victim_ID = 4DF383039AB03953



Victim ID: Offline

The victim ID is created from the following information:

- GUID of the *WindowsDirectory*
- Default UI *Language*
- *OS* version
- Domain Controller
- *Affiliate ID* from the configuration
- *Public key ID* from the configuration

Encodes it using a hard coded 32 character value:

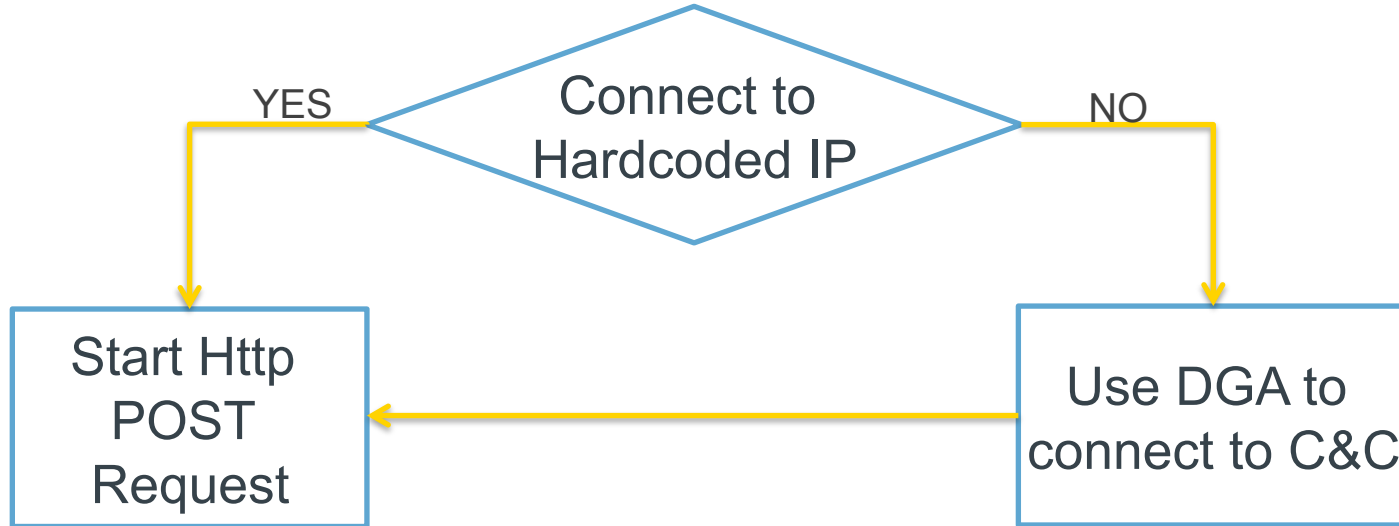
“YBNDRFG8EJKMCPQX0T1UWISZA345H769”.

e.g. victim_ID = IZ8FDGTNEN85I7JZ



C&C Communication

Communication Protocol: C&C



Communication Protocol: Data



Format: *Key* = *value*; Uses & as its delimiter

id=4DF383039AB03953&act=getkey&affid=5&lang=en&corp=0=&serv=0&os=Windows+XP&sp=3&x64=0

Communication Protocol: Data

Format: *Key* = *value*; Uses & as its delimiter

0: not member or a domain
1: member of a domain
2: primary domain controller

Architecture

0: x86
1: x64

Service Pack

id=4DF383039AB03953&act=getkey&affid=5&lang=en&corp=0=&serv=0&os=Windows+XP&sp=3&x64=0

Victim ID

getkey
gettext
gethtml
stats

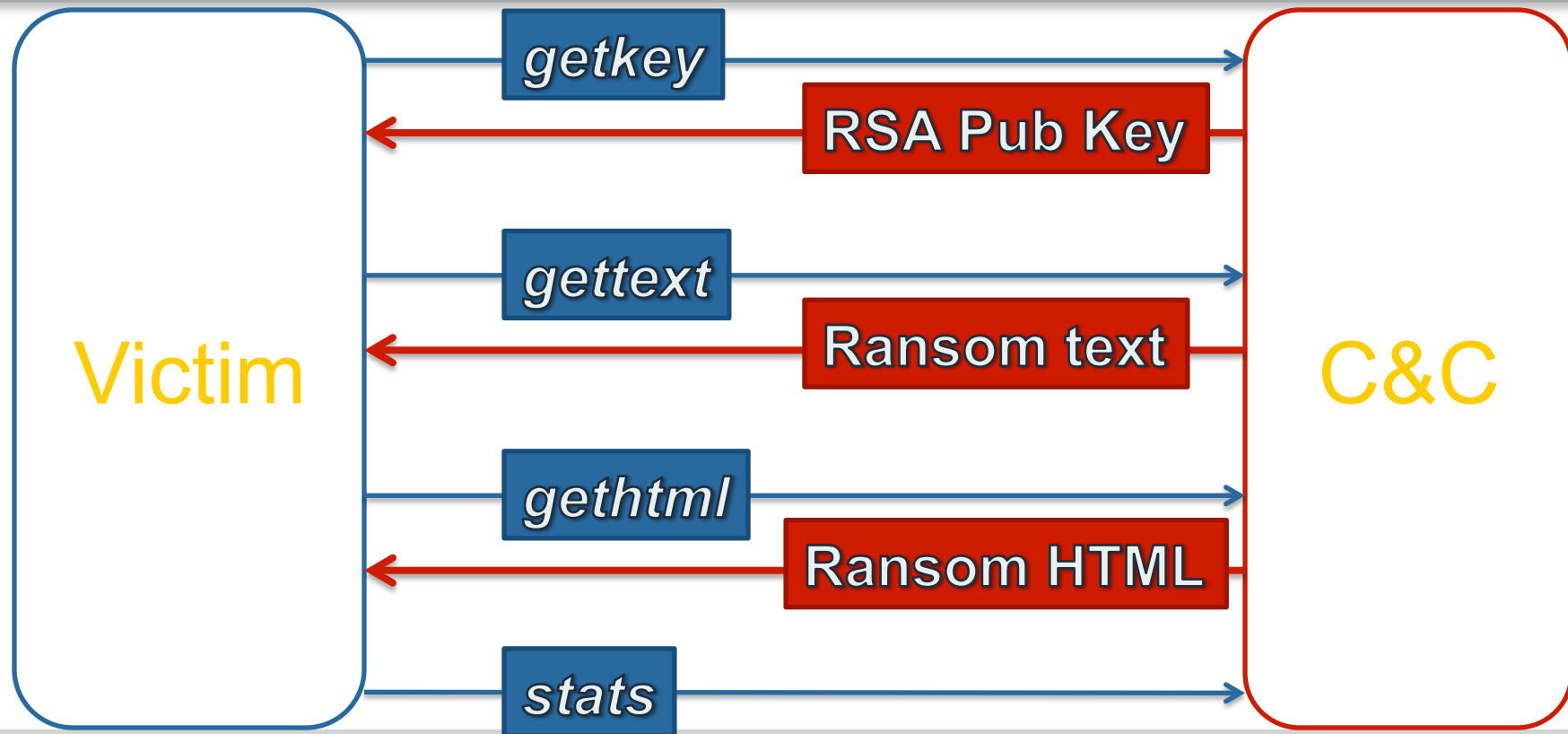
Language

Affiliate ID

Operating System

0: not server
1: server

Communication Protocol: Http request





File Encryption

File Encryption: Targeted drives



- Drive_Removable
- Drive_Fixed
- Drive_Remote
- Drive_Ramdisk

File Encryption: Targeted extensions



Total of 194 file extensions:

.n64, .m4a, .m4u, .m3u, .mid, .wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .mp3, .qcow2, .vdi, .vmdk, .vmx, **.wallet**, .upk, .sav, .re4, .ltx, .litesql, .litemod, .lbf, .iwi, .forge, .das, .d3dbsp, .bsa, .bik, .asset, .apk, .gpg, .aes, .ARC, .PAQ, .tar, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .sh, .class, .jar, .java, .rb, .asp, .cs, .brd, .sch, .dch, .dip, .pl, .vbs, .vb, .js, .h, .asm, .pas, .cpp, .c, .php, .ldf, **.mdf**, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .db, .mdb, **.sql**, **.SQLITEDB**, .SQLITE3, .011, .010, .009, .008, .007, .006, .005, .004, .003, .002, .001, .pst, .onetoc2, .asc, .lay6, .lay, .ms11(Securitycopy), .ms11, .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .pptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wb2, .123, .wks, .wk1, .xltx, .xltn, **.xlsx**, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm, .xlc, .dif, .stc, .sxc, .ots, .ods, **.hwp**, .602, .dotm, .dotx, .docm, **.docx**, .DOT, .3dm, .max, .3ds, .xml, .txt, **.CSV**, .uot, .RTF, **.pdf**, .XLS, .PPT, .stw, .sxw, .ott, .odt, **.DOC**, .pem, .p12, .csr, .crt, .key, **wallet.dat**

File Encryption: Targeted extensions



From 194 to 460 file extensions:

.yuv, .qbx, .nnd, .exf, .cdr4, .vmsd, .dat, .indd, .pspimage, .obj, .ycbcra, .qbw, .mrw, .erf, .cdr3, .vhdx, .cmt, .iif, .ps, .mlb, .xis, .qbr, **.moneywell**, .erbsql, .bpw, .vhd, .bin, .fpx, .pct, .md, .x3f, .qba, .mny, .eml, .bgt, .vbox, .aiff, .fff, .pcd, .mbx, .x11, .py, .mmw, .dxg, .bdb, .stm, .xlk, .fdb, .m4v, .lit, .wpd, **.psafe3**, .mfw, .drf, .bay, .st7, .wad, .dtd, .m, .laccdb, .tex, .plc, .mef, .dng, .bank, .rvt, .tlg, .design, .fxg, .kwm, .sxx, .plus_muhd, .mdc, .dgc, **.backupdb**, .qcow, .st6, .ddd, .flac, .idx, .stx, .pdd, .lua, .des, .backup, .qed, .st4, .dcr, .eps, .html, .st8, .p7c, .kpdx, .der, .back, .pif, .say, .dac, .dxb, .flf, .st5, .p7b, .kdc, .ddrw, .awg, .pdb, .sas7bdat, .cr2, .drw, .dxf, .srw, .oth, .kdbx, **.ddoc**, .apj, .pab, .qbm, .cdx, **.db3**, .dwg, .srf, .orf, .kc2, .dcs, .ait, .ost, .qbb, .cdf, .cpi, .dds, .sr2, .odm, .jpe, .dc2, .agdl, .ogg, .ptx, .blend, .cls, .css, .sqlite, .odf, .incpas, .db_journal, .ads, .nvram, .pfx, .bkp, .cdr, **.config**, .sdf, .nyf, .liq, .csl, .adb, .ndf, .pef, .al, .arw, .cfg, .sda, .nxx, .ibz, .csh, .acr, .m4p, .pat, .adp, .ai, .cer, .sd0, .nx2, **.ibank**, .crw, .ach, .m2ts, .oil, .act, .aac, .asx, .s3db, .nwb, .hbk, .craw, .accdt, .log, .odc, .xlr, .thm, .aspx, .rwz, .ns4, .gry, .cib, .accdr, .hpp, .nsh, .xlam, .srt, .aoi, .rwl, .ns3, .grey, .ce2, .accde, .hdd, .nsg, .xla, .save, .accdb, .rdb, .ns2, .gray, .ce1, .ab4, .groups, .nsf, .wps, **.safe**, **.7zip**, .rat, .nrw, .fhd, .cdrw, .3pr, .flvv, .nsd, .tga, .rm, .1cd, .raf, .nop, .fh, .cdr6, .

3fr, .edb, .nd, .rw2, .pwm, .wab, .qby, .nk2, .ffd, .cdr5, .vmxf, .dit, .mos, .r3d, .pages, .prf, .oab, .msg, .mapima

35 il, .jnt, .dbx, .contact

File Encryption: Algorithm



Encryption used:

- Uses both **RSA** and **AES** algorithms
- The **AES-128** key is randomly generated for each file
- The **AES-128** key is used to encrypt the file and its filename
- After encryption, the **AES-128** key will be encrypted by **RSA-2048**

File Encryption: Filename



Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID

File ID

File Encryption: Filename



Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID

File ID

0X3U7IYC-IA09-CQ94-D26F-CFA67B8E895D.zepto

Victim ID

File ID

File Encryption: Filename



Format of filenames of encrypted files.

4DF383039AB03953D81660EB4CADC28D.locky

Victim ID

File ID

0X3U7IYC-IA09-CQ94-D26F-CFA67B8E895D.zepto

Victim ID

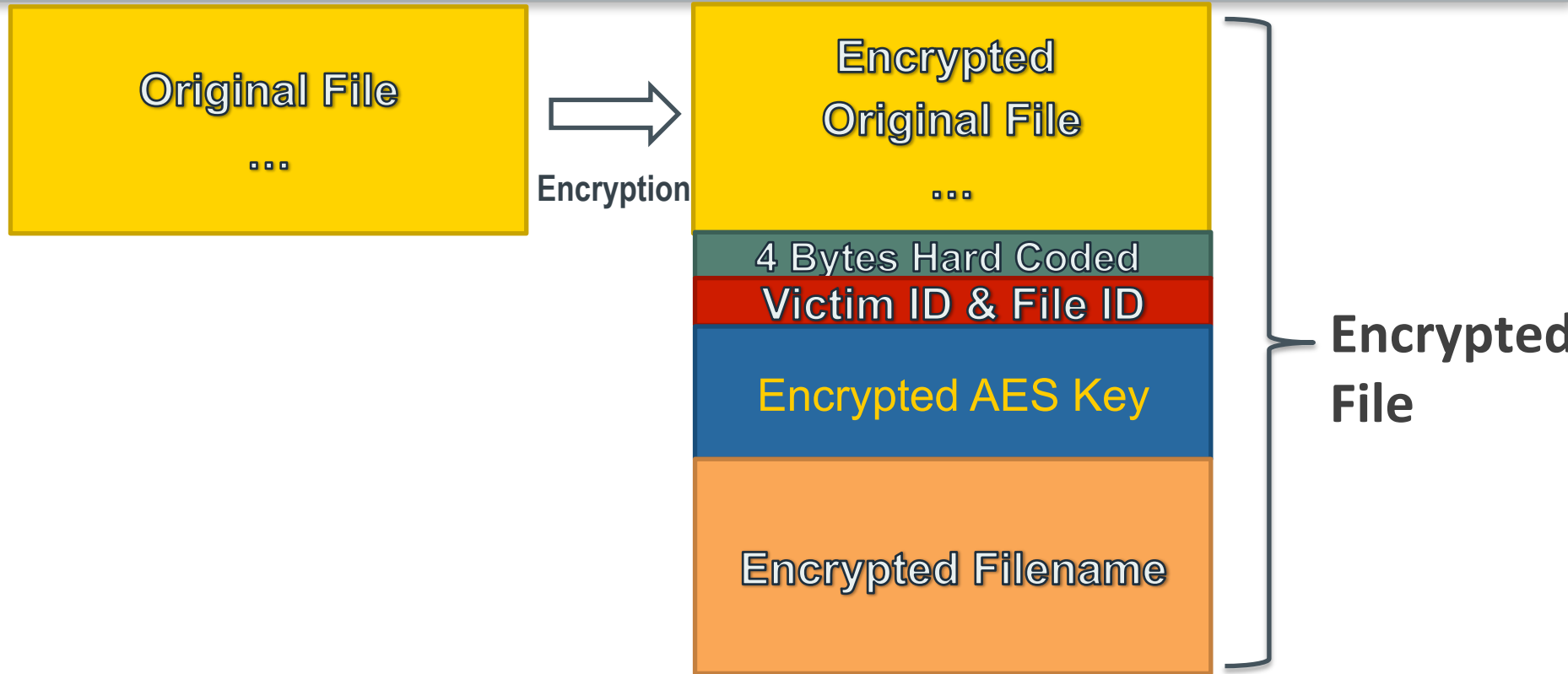
File ID

0X3U7IYC-IA09-CQ94-D26F-CFA67B8E895D.odin

Victim ID

File ID

File Encryption: File layout



File Encryption: File layout

```
0000000A2: A2 7F 33 AF 28 3B 88 23 11 C2 A5 69 D1 12 06 53 6A3><;e#4rNi:†$S
0000000B2: C9 15 96 55 7B 5B 49 60 A5 89 11 82 9E 67 65 63 fSÜÜ<LI Nê4érgec
0000000C2: 66 F3 65 8C 5E A4 AB D0 A3 1C 6B 94 AC 93 8E A0 fSei^ñ^u-kü%öäa
0000000D2: 84 4B 6B D8 A4 A9 BC A4 CF BA 49 5A B2 8D 42 13 äKk+ñ-ñ±||Z||B!!
0000000E2: B9 C5 58 68 3D FA 05 C2 D8 57 FF F7 63 14 FA 8B ||tXh=->1TÜ scq-i
0000000F2: FA CA 31 99 C0 95 A2 A3 36 2B 48 52 52 74 1F 02 -10↳öü6+HRRtV@
000000102: E7 10 D0 F1 7D 91 42 56 F8 67 FE CA 4E 2C 4D B3 rU+>æBU°g~N|M|
000000112: B8 06 3E 31 09 97 F1 E1 8A C2 49 EF B3 8D F4 10 >1Öü±β±TIn|i|
000000122: 3F 5B 7F 39 18 8D 0A 1F BE 80 01 B7 32 B0 BE 57 ?[Δ9†iÖV°C@n2|W
000000132: E7 92 EF 3A 28 3F 74 50 40 AE 2A D8 F7 BD 28 21 rññ:~?tP@<×~>|<
000000142: 8C 14 23 BF 53 6D 4E D7 17 E3 3D 32 8A 56 4A 4F iññ-SmN|||±=2èUJO
000000152: A7 21 6D B2 E0 A0 19 6B 8C 03 9D 20 6B 2F 64 DC e°m/αá1k3w k/d~
000000162: D7 06 14 B4 B6 A3 D9 24 A3 9B 8C D6 26 86 38 EA ||+ñ||ü°$úçíñ&á8ñ
000000172: 22 F5 CB 3F 2B 5D 1B 24 7E A4 55 0B 5E 3F E2 DC "J~+1<$~ñÜδ^?Γ
000000182: F5 C4 B1 81 42 99 96 60 A8 B3 05 9D F4 4B 9F EE J-üB00°&|~V°KfE
000000192: D4 1B 15 53 05 0F 34 99 41 F9 51 07 86 DA 90 78 t=SSα40ñ-Q-á.réx
0000001A2: E1 84 9A 3E 5F BC FD CF BA F3 50 D1 93 FE 56 89 BñÜ>~±||sP-6IÜ@
0000001B2: 34 44 46 33 38 33 30 33 39 41 42 30 33 39 35 33 4DF383039AB03953
0000001C2: 66 35 82 F1 36 1A 64 92 7A C1 66 F3 A4 E0 4D E8 rSe±b>dkz-†±ñαñg
0000001D2: 3F 98 2F 68 8E 24 F8 DD B1 75 A0 6B E7 24 4A 8B ?y/há$°||uákr$ññ
0000001E2: 31 79 65 73 1D 8A 06 93 96 37 F6 6D 49 E1 AC FE 1yes+æ±öü7±mIβ%ñ
0000001F2: 47 DC 47 62 26 BC 2A 05 83 FE 3A CA 40 2B 2B B5 G-Gb&~±αá||:~ö+~+~
000000202: 8A 39 99 FD 11 B2 0A 36 29 A9 C5 FF 24 65 43 27 è90°~<06°>~+~$eC
000000212: C7 24 82 D6 33 9E D3 C7 5E 1B B7 7E EF 1D 47 F0 ||$éñ3KÜ||~+~ñ~+G~
000000222: 3F F0 DB 36 9E A6 A0 27 39 3F 7D 47 66 F7 55 B9 ?=±6Rαá°9?>GfñÜ||
000000232: 06 7F 78 60 6D CE 95 25 64 D7 9F 4C A9 B0 61 CD αα~m||ö±d||fLr~a=
000000242: B7 21 95 66 77 42 98 25 69 0C 84 8A E3 8A B0 84 ñ°öföBÜ°iVæññ~ä
000000252: EE C8 E9 B8 B6 DB D6 F2 1C 06 23 41 81 FD 78 A2 €L9q||~ñ±~±ñü±xö
000000262: 3B CB CF 5A 6D A2 49 6B 8A DB C3 A3 59 19 52 22 ~ZmóIkè~|üVJr~
000000272: 9C B1 86 3B 92 77 F8 21 79 2A 5E FD AF 94 DE 82 f~ä;ñw°°y~×~±öñ6
000000282: AF 6F D0 46 DF 07 8F EC 8C 05 81 59 5B 79 C4 6D >xoüF~°8wñüVly-m
000000292: 1C 06 69 09 93 CE 7C 60 3C CD B8 E7 96 A0 27 3C ~iöô||~<~rÜá°<
0000002A2: FF E6 B3 F6 CA 26 1A 7B 07 94 85 64 C4 FF 2F EA µ||÷~&~<~öä~°/ñ
0000002B2: 2F F1 7F 29 8F 9B F8 22 0A 5E D0 CE 37 75 E4 78 /±α>8ç°||~ñü7uEx
0000002C2: 42 F9 B1 2D 6C B2 92 67 DC BB 7B 8B 78 B9 12 51 B-~1ñ9~ñ<1x||+ü
0000002D2: DD 1F 8D 31 27 02 E1 E6 3E 02 75 75 CD 79 50 13 |V1°~0µ>Öuu=yP||
0000002E2: F2 BC 08 11 C7 97 D9 5A CB 49 79 36 79 CD 2A 47 èJÖ||ñJ2rIy6y~×G
0000002F2: 0A D9 E5 1D 96 0A BA 81 86 79 61 E3 92 5F 30 94 C°±o±ü||üäyallñ~00
000000302: 1B 4D 5B 6E 27 F0 B8 05 AC C8 0F 06 22 0E 59 BA ~MIn°~±~±~±~°~ñV||
000000312: D9 4C 36 2D 9B E5 81 43 F4 3C 98 A4 DD 9E 3D DA JL6-çöüC<Yñ||R=ñ
000000322: 73 AD B3 4E 0F 07 8D F2 38 70 09 8E EC 48 17 B7 s:|N×~±è8pöñwñH±ñ
000000332: CD 07 DC E9 BC C6 5A 7D 16 16 7E 20 14 EC 22 86 ~°~ñJZ~°~ñw~ä
000000342: 05 4F 26 39 E6 BB BB 5B A7 5F 68 3A F8 59 9C αO89µñ||±~h4:oyf
000000352: 12 CC 9D C4 6A B5 87 B1 11 5D 99 E1 DC 40 57 89 ð|ñ~jñç~100~öwE
000000362: BB C2 B6 81 8A E5 0E 6B B7 7A 17 2F F7 5E 61 1A ññ||üèöñkñ±~ñ~a~
000000372: CB 32 2A EF 88 F8 5B CF DC D2 D7 17 D3 D1 25 37 ~2~ñè°||~ññ||~ñ~
000000382: 11 E2 3A 24 3E 0C 53 B2 24 1F 30 A5 DC 4A 93 AE <ñ:~$>QS~ñVññJö<<
```

Encrypted Data

*Encryption used:

AES-128

Hardcoded Value

Victim ID & File ID

Encrypted AES Key

*Encryption used:

RSA-2048

Encrypted Filename

*Encryption used:

AES-128

HTML Ransom Note



```
i»¿|.+=+=$-=-..-.___=
=-...$$|= $$=+*
```

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:

1. <http://5n7y4yihirccftc5.tor2web.org/ECCEADDE847A1F1A>
2. <http://5n7y4yihirccftc5.onion.to/ECCEADDE847A1F1A>

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 5n7y4yihirccftc5.onion/ECCEADDE847A1F1A
4. Follow the instructions on the site.

!!! Your personal identification ID: ECCEADDE847A1F1A !!!

```
*+$-==+=+_
```

```
_ + .+--. ..|++=$-+=
```

Decryptor Page

Languages:

Locky Decryptor™

We present a special software - **Locky Decryptor™** - which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

1

You can make a payment with BitCoins, there are many methods to get them.

2

You should register BitCoin wallet:
[Simplest online wallet](#) or [Some other methods of creating wallet](#)

3

Purchasing Bitcoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.

Here are our recommendations:

[localbitcoins.com \(WU\)](#)
[coincafe.com](#)

[localbitcoins.com](#)
[cex.io](#)
[btcdirect.eu](#)
[bitquick.co](#)
[howtobuybitcoins.info](#)
[cashintocoins.com](#)
[coinjar.com](#)
[anxpro.com](#)
[bittylicious.com](#)

Buy Bitcoins with Western Union.
Recommended for fast, simple service.
Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
Service allows you to search for people in your community willing to sell bitcoins to you directly.
Buy Bitcoins with VISA/MASTERCARD or wire transfer.
The best for Europe.
Buy Bitcoins instantly for cash.
An international directory of bitcoin exchanges.
Bitcoin for cash.
CoinJar allows direct bitcoin purchases on their site.

4

Send **0.5 BTC** to Bitcoin address:

Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

Date	Amount BTC	Transaction ID	Confirmations
		not found	

5

Refresh the page and download decryptor.

When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.

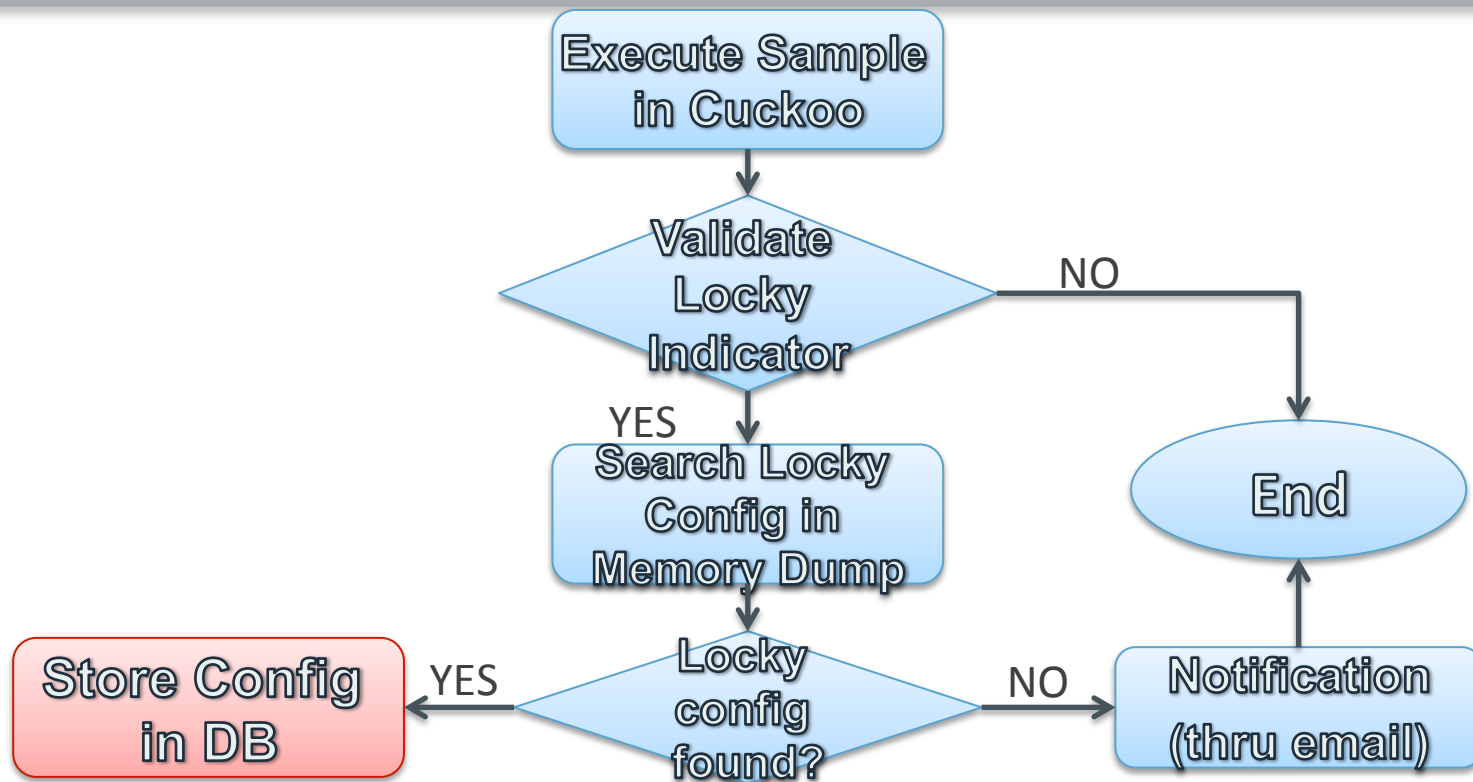


Harvest Locky Configuration

Automate Configuration Extraction: Overview



Cuckoo Setup





Demo: Locky

Config Extraction in

Cuckoo Sandbox

Takeaways





Thank you



fbacurio@fortinet.com
rjoen@fortinet.com



[@fbacurio](#)
[@rommeljoen17](#)